

WHAT IS CLAIMED IS:

1. A programming interface on a mobile device for transferring information to and from a radio receiver on the mobile device, the programming interface including:

a message processing component configured to receive messages to be delivered to the radio receiver; and

a driver component coupled to the message processing component;

wherein the message processing component is configured to execute a control call to the driver component specifying a control operation to be performed based on a message received, an input buffer location of an input buffer containing data to be transferred to the radio receiver, a number of bytes of information contained in the input buffer, an output buffer location of an output buffer containing information received from the radio receiver, a maximum number of bytes of information contained in the output buffer, and an actual number of bytes received from the radio receiver; and

wherein the driver component is configured to receive the control call from the message processing component and execute the specified control operation.

2. The programming interface of claim 1 wherein

the control operation is a programming operation to program values in the radio receiver and wherein the control call passes a programming data structure to the driver, the programming data structure including:

- a structure size portion indicative of a size of the programming data structure;
- a mask portion indicative of which portions in the programming data structure are valid;
- an operation code portion indicative of whether the programming operation is to program values or deprogram values;
- a type code portion indicative of a type of values to be programmed or deprogrammed;
- a program data portion indicative of the values to be programmed or deprogrammed;
- and
- a program data length portion indicative of a length of the program data.

3. The programming interface of claim 2 wherein the type code portion is indicative of an encryption key to be programmed or deprogrammed and wherein the program data portion comprises a key data structure.

4. The programming interface of claim 3 wherein the key data structure includes:

- a structure size portion indicative of a size of the key data structure;
- a mask portion indicative of which portions of the key data structure are valid;
- a key portion indicative of the encryption key;
- a key number portion indicative of a number

corresponding to the encryption key;
an algorithm portion indicative of an encryption algorithm to be used in conjunction with the encryption key;
a key length portion indicative of a length of the encryption key;
a key tag portion indicative of a location in which the encryption key is stored; and
a key tag length portion indicative of a length of the key tag portion.

5. The programming interface of claim 2 wherein the mobile device receives messages over an address and wherein the type code portion is indicative of an address to be programmed or deprogrammed and wherein the program data portion comprises an address data structure.

6. The programming interface of claim 5 wherein the address data structure includes:

a structure size portion indicative of a size of the address data structure;
a mask portion indicative of which portions of the address data structure are valid;
an address portion indicative of the address;
an address number portion indicative of a number corresponding to the address;
a status portion indicative of a status of the address;
an address tag portion indicative of a tag associated with the address portion;
an expiration date portion indicative of an expiration date associated with the

address, wherein subsequent messages received over the address after the expiration date are discarded; and an address tag length portion indicative of a length of the address tag portion.

7. The programming interface of claim 6 wherein the address data structure further includes:

a key tag portion indicative of a location at which an encryption key used to decrypt messages received over the address is stored; and

a key tag length portion indicative of a length of the key tag portion.

8. The programming interface of claim 6 wherein the address data structure further comprises:

an address name portion indicative of a descriptive name of the address;

a description portion indicative of a textual description of messages received over the address;

an address name length portion indicative of a length of the address name portion; and

a description length portion indicative of a length of the description portion.

9. The programming interface of claim 2 wherein the mobile device receives messages over an address and a group code corresponding to the address and wherein the type code portion is indicative of a group code to be programmed or deprogrammed and wherein the program data portion comprises a group code data

structure.

10. The programming interface of claim 9 wherein the group code data structure includes:

- a structure size portion indicative of a size of the group code data structure;
- a mask portion indicative of which portions of the group code data structure are valid;
- an group code portion indicative of the group code;
- an group code number portion indicative of a number corresponding to the group code;
- a status portion indicative of a status of the group code;
- an expiration date portion indicative of an expiration date associated with the group code, wherein subsequent messages received over the group code after the expiration date are discarded;
- a group code tag portion indicative of a tag associated with the group code;
- an address tag portion indicative of a tag associated with the address;
- an address tag length portion indicative of a length of the address tag portion; and
- a group tag length indicative of a length of the group tag portion.

11. The programming interface of claim 10 wherein the group code data structure further includes:

- a key tag portion indicative of a location at which an encryption key used to decrypt messages received over the group code is

stored; and
a key tag length portion indicative of a
length of the key tag portion.

12. The programming interface of claim 11 wherein
the group code data structure further comprises:

a group code name portion indicative of a
descriptive name of the group code;
a description portion indicative of a textual
description of messages received over the
group code;
an group code name length portion indicative
of a length of the group code name
portion; and
a description length portion indicative of a
length of the description portion.

13. The programming interface of claim 2 wherein
the mobile device receives messages over an address
from a carrier and wherein the type code portion is
indicative of a carrier designation to be programmed
or deprogrammed and wherein the program data portion
comprises a carrier data structure.

14. The programming interface of claim 13 wherein
the carrier data structure includes:

a structure size portion indicative of a size
of the carrier data structure;
a mask portion indicative of which portions of
the carrier data structure are valid;
a frequency portion indicative of a radio
frequency at which the messages are
received from the carrier;

a name portion indicative of a name of the carrier;
a description portion indicative of a description of message types received from the carrier;
a user identification portion indicative of an identification number associated with a user of the mobile device;
an user identification length portion indicative of a length of the user identification portion;
a name length indicative of a length of the name portion; and
a description length portion indicative of a length of the description portion.

15. The programming interface of claim 2 wherein the radio receiver has existing values stored therein, wherein programming data portion comprises a programming data structure having a plurality of fields, each field corresponding to a value on the radio receiver and each field containing new values to be programmed into the radio receiver, and wherein existing values on the radio receiver are left unchanged when the field in the programming data structure does not have a field corresponding to the existing value.

16. The programming interface of claim 1 wherein the wherein the driver component includes:

a function library of functions performed by the driver in executing the specified control operation.

17. The programming interface of claim 16 wherein the function library includes:

an encryption key derivation component for deriving an encryption key based on information provided to the driver component in the control call, wherein the driver component utilizes the encryption key derivation component to derive the encryption key, stores the encryption key at a key location in the driver component and returns a key handle indicative of the key location to the message processing component.

18. The programming interface of claim 16 wherein the function library includes:

a decryption and validation component for decrypting and validating information provided to the driver component in the control call, the driver component utilizing the decryption and validation component to decrypt and validate the information and returning a value to the message processing component indicative of whether the information is valid.

19. The programming interface of claim 1 wherein the driver component is configured to return a value to the message processing component indicative of whether the control operation specified by the control call has been performed.

20. A computer readable medium on a mobile device, the computer readable medium having a first data structure stored thereon, the first data structure comprising:

- an address information portion indicative of an address over which the mobile device receives messages;
- an address tag portion indicative of a tag associated with the address portion;
- an expiration date portion indicative of an expiration date associated with the address, wherein subsequent messages received over the address after the expiration date are discarded;
- a key index portion indicative of a location on the computer readable medium storing an encryption key associated with the messages received over the address; and
- a status portion indicative of a status of the address.

21. The computer readable medium of claim 20 wherein the status portion is indicative of whether the address is enabled.

22. The computer readable medium of claim 20 wherein the status portion is indicative of whether messages received over the address have a predetermined priority indicative of a time within which the messages are processed.

23. The computer readable medium of claim 20 wherein the status portion is indicative of whether a

Sub
B1

B1
message received over the address are enabled only under predetermined power conditions.

24. The computer readable medium of claim 20 wherein the first data structure includes:

an address name portion indicative of a descriptive name of the address.

25. The computer readable medium of claim 20 wherein the first data structure includes:

a description portion indicative of descriptive text describing the messages received over the address.

26. The computer readable medium of claim 20 and further comprising a second data structure stored on the mobile device, the second data structure including:

an encryption key portion indicative of an encryption key used to decrypt a received message;

an encryption algorithm portion indicative of an encryption algorithm used to encrypt the message; and

a key tag portion indicative of a key tag associated with the encryption key.

27. The computer readable medium of claim 26 and further comprising a third data structure stored on the mobile device, the third data structure including:

a service group code portion indicative of a service group code over which the mobile device receives messages;

- B1
- a status portion indicative of a status of the service group code;
 - a key index portion indicative of a location on the computer readable medium which stores an encryption key associated with the messages received over the service group code;
 - an expiration date portion indicative of an expiration date associated with the service group code, wherein subsequent messages received over the service group code after the expiration date are discarded; and
 - a service group tag indicative of a tag associated with the service group code.

28. The computer readable medium of claim 27 wherein the mobile device includes a radio receiver and wherein the first, second and third data structures are stored on the radio receiver.

29. A computer readable medium on a mobile device, the computer readable medium having a data structure stored thereon, the data structure comprising:

- an encryption key portion indicative of an encryption key used to decrypt a received message;
- an encryption algorithm portion indicative of an encryption algorithm used to encrypt the message; and
- a key tag portion indicative of a key tag associated with the encryption key.

30. The computer readable medium of claim 29 wherein the mobile device includes a radio receiver and wherein the data structure is stored on the radio receiver.

31. A computer readable medium on a mobile device, the computer readable medium having a data structure stored thereon, the data structure comprising:

- a service group code portion indicative of a service group code over which the mobile device receives messages;
- a status portion indicative of a status of the service group code;
- a key index portion indicative of a location on the computer readable medium which stores an encryption key associated with the messages received over the service group code;
- an expiration date portion indicative of an expiration date associated with the service group code, wherein subsequent messages received over the service group code after the expiration date are discarded; and
- a service group tag indicative of a tag associated with the service group code.

32. The computer readable medium of claim 31 wherein the data structure comprises:

- a service group name portion indicative of a descriptive name for the service group code.

33. The computer readable medium of claim 31 wherein the data structure comprises:

a description portion indicative of descriptive text describing messages received over the service group code.

34. The computer readable medium of claim 31 wherein each service group code they have associated addresses and are stored in a location arranged according to the address and then according to service group code.

35. The computer readable medium of claim 31 wherein the mobile device includes a radio receiver and wherein the data structure is stored on the radio receiver.

36. The computer readable medium of claim 31 wherein the computer readable medium includes a key table and wherein the key index is indicative of a location in the key table which holds the encryption key.

37. A transmission system for transmitting information from an originator to a mobile device, the transmission system comprising:

an originator component configured to receive the information to be transmitted and form a transmission message; and
a receiver component configured to receive the transmission message;

wherein the originator includes:

a first encryption key component

configured to derive a first encryption key based on a base key known by the receiver component, a first data string and a data portion including message specific data derived from the information to be transmitted;

a second encryption key component configured to derive a second encryption key based on the base key, a second data string and the data portion;

an encryptor configured to hash the information to be transmitted with the first encryption key to obtain a signature and to encrypt the information and the signature with the second encryption key to obtain an encrypted message; and

a joiner configured to join the encrypted message with the message specific data, in unencrypted form.

38. The transmission system of claim 37 wherein the originator comprises:

a header generation component configured to receive the encrypted message and message specific data and add a header thereto to obtain the transmission message.

39. The transmission system of claim 37 wherein the first encryption key component hashes the base key, the first data string and the message specific

data to obtain a bias value and wherein the first encryption key component includes:

a key generator configured to receive the bias value and generate the first encryption key based on the bias value.

40. The transmission system of claim 37 wherein the second encryption key component hashes the base key, the second data string and the message specific data to obtain a bias value and wherein the second encryption key component includes:

a key generator configured to receive the bias value and generate the second encryption key based on the bias value.

41. The transmission system of claim 37 wherein the originator includes:

a checksum component configured to calculate a checksum over the transmission message and append the checksum thereto.

42. The transmission system of claim 41 wherein the receiver component comprises:

a processor component; and
a driver component coupled to the processor component;

wherein the processing component is configured to receive the transmission message and pass the transmission message to the driver component, the driver component being configured to derive the first and second encryption keys from the based key, the first and second data strings

and the message specific data and decrypt the transmission message.

43. The transmission system of claim 42 wherein the driver component further comprises:

a validation component configured to calculate a checksum over the unencrypted transmission message, and compare the checksum calculated to the checksum calculated by the checksum component to determine whether the unencrypted message is valid.

44. The transmission system of claim 37 wherein the mobile device includes a radio receiver having values stored therein, the values determining operation of the radio receiver, and wherein the transmission message comprises a programming message for programming the values in the radio receiver.

45. A wireless transmission system for transmitting programming data to a mobile device having a one-way radio receiver thereon, the transmission system including:

an originator component configured to receive the programming data and form a programming message indicative of the programming data;

a transmitter component, selectively coupleable to the originator, configured to transmit the programming message to the mobile device;

a mobile device processing component

configured to receive the programming message and provide it to the radio receiver and to provide an acknowledge message in response to successfully providing the programming message to the radio receiver;

a mobile device synchronization component coupled to the mobile device processing component;

a desktop computing device selectively coupleable to the mobile device and including a desktop synchronization component operable with the mobile device synchronization component to synchronize the acknowledge message to the desktop computing device; and

a desktop communication component selectively coupleable to the originator and configured to pass the acknowledge message to the originator.

46. The wireless transmission system of claim 45 wherein the transmitter component comprises:

an originator communication component selectively coupleable to the desktop communication component and configured to transmit the programming message to the desktop computing device for synchronization to the mobile device processing component.

47. The wireless transmission system of claim 45 wherein the transmitter component comprises:

a radio transmitter configured to broadcast the programming message to the radio receiver.

48. The wireless transmission system of claim 45 wherein the transmitter component comprises:

a modem configured to transmit the programming message to the radio receiver.

49. The wireless transmission system of claim 45 wherein the transmitter component comprises:

a portable magnetic storage medium, readable by the mobile device processing component, storing the programming message.

50. The wireless transmission system of claim 45 wherein the desktop communication component comprises a global computer network browser.